UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/500,311	06/28/2004	David Arditti Modiano	T2678-9156US01	9860

181 7590 10/29/2008

MILES & STOCKBRIDGE PC
1751 PINNACLE DRIVE
SUITE 500
MCLEAN, VA 22102-3833

EXAMINER	
YALEW, FIKREMARIAM A	

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
10/29/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ipdocketing@milesstockbridge.com
sstiles@milesstockbridge.com

Office Action Summary	Application No.	Applicant(s)	
	10/500,311	ARDITTI MODIANO ET AL.	
	Examiner	Art Unit	
	Fikremariam Yalew	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 July 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *19,21,23-36,39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *19,21,23-36,39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The office action is in replay to an amendment filed on 07/14/2008.Claims 19,23,33-36, 39 have been amended. Claims 1-18,20,22,37-38 and 40 were previously canceled. Claims 19,21,23-36,39 are pending.

Response to Arguments

2. Applicant's arguments with respect to claim 19,21,23-36,39 have been considered but are moot in view of the new ground(s) of rejection.

Priority

2. Acknowledgment is made of Applicant claim for foreign priority under 35 U.S.C 119(a)-(d) ,for the benefit of the filing date of the corresponding French Patent application no.01/16950 filed on 27 December 2001.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 19,21,23-36,39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hopkins et al (hereinafter referred as Hopkins) US Patent 7,093,133 B2 in view of Inada(US Patent No 6,986,044 B1).

6. As per claim 19: Hopkins disclose a group signature device for providing a message (m) accompanied a group by a group signature (S) comprising means storing personalized data(z, Kz) identifying an individual member(M) of a group(G)(See Fig 2 and col 6 lines 38-56 and col 6 lines 9-22); encryption means(B3)for producing an encrypted text(C)(See col 6 lines 61-63 and col 8 lines 23-30),intended to be associated with said message (m),using said personalized data (z,Kz)(See col 6 lines 38-63 and col 8 lines 23-30); singing means (B6) for producing the group signature (S) with a private signature key (SK) common to all group members using the message to be signed (m) and said encrypted text (C)(See Fig 7 step 20 and col 5 lines 23-35); and means for outputting the message (m) and the group signature (S) to a checker, such that the checker, upon receiving the message accompanied by the group signature, is able to verify that message(m) is associated with the group (G) based on the group signature (S), with the identify of the member (M) of the group (G) remaining anonymous the checker(See col 2 lines 52-57 and col 5 lines 36-56).

Hopkins does not explicitly teach an encrypted text(c) produced using the personalized data(z,Kz) of said individual member (M) only(See col 8 lines 1-9 and Fig 3 step 3,Fig 7).

However Inada teaches an encrypted text(c) produced using the personalized data(z,Kz) of said individual member (M) only(See col 8 lines 1-9 and Fig 3 step 3,Fig 7).

Therefore it would have been obvious to one having ordinary skill in the art at that time the invention was made to employ the teaching method of Inada within Hopkins method inorder to provide a signature system which enables an arbitrary member who belongs a specific group to write a signature and to verify that a signature on a signed document is the signature written by a member who belongs to the specific group (See Inada col 2 lines 40-43)

8. As per claim 21: the combination of Hopkins and Inada disclose a group signature device further comprising means (B5) for combining the message (m) to be signed and the encrypted text (C) associated with said message (m) in the form of a concatenation of the message (m) with the encrypted text (C)(See Hopkins col 6 lines 61-63 and col 8 lines 23-30 and Fig 7 steps 100,20).

9. As per claim 23: the combination of Hopkins and Inada disclose a group signature device wherein said personalized data is an identifier (z) personal to the member (M), said means for storing further includes an encryption key (K) common to all members of the group (G), and encryption means (B3) produces said encrypted text(C) using the identifier (z) and said encryption key (K) (See Hopkins col 5 lines 18-35 and col 10 lines 11-38).

10. As per claim 24: the combination of Hopkins and Inada disclose a group signature device in which encryption means (B3) produces said encrypted text (C) using identifier (z) and a random number (r)(See Hopkins col 7 lines 31-38 and col 10 lines 1-10).

11. As per claim 25: the combination of Hopkins and Inada disclose a group signature device wherein said personalized data is a diversified encryption key (Kz) specific to each member (M) of the group (G), and encryption means (B3) produces said encrypted text (C) using at least one data and said diversified encryption key (Kz) (See Hopkins col 5 lines 18-35 and col 10 lines 11-38).

12. As per claim 26: the combination of Hopkins and Inada disclose a group signature device wherein said data includes a random number(r) (See Hopkins col See col 7 lines 31-38 and col 10 lines 1-10).

13. As per claim 27: the combination Hopkins and Inada disclose a group signature device wherein the encryption means (B3) uses a secret key encryption algorithm(K)(See Hopkins 10 lines col 26-38).

14. As per claim 28: the combination of Hopkins and Inada disclose a group signature device wherein the encryption means (B3) uses one of the Rivest, Shamir, Adleman or Advanced Encryption Standard (AES) public encryption algorithms (See Hopkins 10 lines col 26-38).

15. As per claim 29: the combination of Hopkins and Inada disclose a group signature device wherein the sign means (sig-B6) uses a private key signature algorithm (SK) (See Hopkins 10 lines col 26-38).

16. As per claim 30: the combination of Hopkins and Inada disclose a group signature device which the private key signature algorithm is of Rivest, Shamir, Adleman(RSA) type.(See Hopkins col 10 lines col 26-38).

17. As per claim 31: the combination of Hopkins and Inada disclose a group signature device in which said group signature device is a portable communicating device (26)(See Hopkins col 6 lines 9-18).

18. As per claim 32: the combination of Hopkins and Inada disclose disclose a group signature device in which said portable communicating device is a smart card (26)(See Hopkins col 6 lines 9-18).

19. As per claim 33: Hopkins discloses a method for secure communication of a message (m) sent by an individual a member (M) of a group (G) using a group a signature (S) the method comprising producing the group signature (S) of the message (m) by singing, with a private signature key (SK) common to all group members (M), a set including the message (m) and

encrypted text(C) produced by using a personalized data (Z, Kz)(See col 5 lines 18-35 and col 10 lines 11-38); and outputting the message(m) along with the group signature (S)(See Fig 7 step 20)

Hopkins does not explicitly teach an encrypted text(c) produced using the personalized data(z,Kz) of said individual member (M) only.

However Inada teaches an encrypted text(c) produced using the personalized data(z,Kz) of said individual member (M) only(See col 8 lines 1-9 and Fig 3 step 3,Fig 7).

Therefore it would have been obvious to one having ordinary skill in the art at that time the invention was made to employ the teaching method of Inada within Hopkins method inorder to provide a signature system which enables an arbitrary member who belongs a specific group to write a signature and to verify that a signature on a signed document is the signature written by a member who belongs to the specific group (See Inada col 2 lines 40-43)

20. As per claim 34: the combination of Hopkins and Inada disclose the method further comprising using a public key (PK) corresponding to said private signature key(SK),that the message (m) is associated with the group(G) based on the group signature (S), without identifying the individual member(M) of the group (G)(See Hopkins col 2 lines 53-57 and col 5 lines 48-56)

21. As per claim 35: the combination of Hopkins and Inada disclose the method further comprising the steps of: decrypting the encrypted text (C) thus obtaining the personalized data (z, Kz)(see col 5 lines 38-41); and identifying the member (M) of the group (G) based on said personalized data (z, Kz)(See Hopkins col 5 lines 41-56 and col 6 lines 5-18).

22. As per claim 36: the combination of Hopkins and Inada disclose the method further comprising producing a private signature key(SK) common to all members of group(G); producing personalized data (z; Kz) identifying the member (M) accepted into group (G)(See Fig 2 and col 6 lines 38-56 and col 6 lines 9-22); and registering said personalized data (z, Kz) with the private signature key(SK) in an electronic device personalized to said member (M) of the group (G)(See Hopkins Fig 2 and col 6 lines 38-56 and col 6 lines 9-22)

23. As per claim 39: Hopkins discloses a group signature system for ensuring a secure communication of a message (m) sent by individual a member (M) of a group (G) using a group signature (S), said group signature system comprising; an electronic device configured to store a personalized data (z, Kz) identifying the individual member (M) of the group (G)(See Fig 2 and col 6 lines 38-56 and col 6 lines 9-22), to produce the group signature (S) with a private key (SK) common to all group members using the message (m) and said encrypted text(C) and to output the message(m) and the group signature(S)(See Fig 7 step 20 and col 5 lines 23-35); a checker that receives that receives the message (m) accompanied by the group signature (S) output from the electronic device, said checker being configured to verify that the message (m) is associated with the group signature (G) based on the group singnature(S), the identity of the member (M) remaining anonymous to the checker(See col 2 lines 52-57 and col 5 lines 36-56); and a trusted authority configured to identify the member(M) of the group(See Fig 1 step 14)

Hopkins does not explicitly teach an encrypted text(c) produced using the personalized data(z,Kz) of said individual member (M) only.

However Inada teaches an encrypted text(c) produced using the personalized data(z,Kz) of said individual member (M) only(See col 8 lines 1-9 and Fig 3 step 3,Fig 7).

Therefore it would have been obvious to one having ordinary skill in the art at that time the invention was made to employ the teaching method of Inada within Hopkins method inorder to provide a signature system which encables an arbitrary member who belongs a specific group to write a signature and to verify that a signature on a signed document is the signature written by a member who belongs to the specific group (See Inada col 2 lines 40-43)

Conclusion

24. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser,can be reached on 5712738300. The fax phone number for the organization where this application or proceeding is assigned is 571-272-4195.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should
you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Fikremariam Yalew
10/23/2008
FA

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436